Autonomous Threat Intelligence Aggregator: Leveraging AI for Real-Time Cyber Threat Detection and Response

Anurag Pathak
Department of Computer Science, B.Tech GLA University, Mathura, Uttar Pradesh, India

Arpit Sharma
Department of Computer Science, B.Tech GLA University, Mathura, Uttar Pradesh, India

Abstract

As cyber threats grow in complexity, traditional security mechanisms struggle to provide timely responses. This paper introduces the Autonomous Threat Intelligence Aggregator (ATIA), an AI-driven system for real-time cyber threat detection, classification, and mitigation. ATIA employs Natural Language Processing (NLP) to extract Indicators of Compromise (IoCs) from unstructured sources, while Machine Learning (ML) models classify risks and enhance threat assessment. Integrated with Security Information and Event Management (SIEM), ATIA automates responses, reducing manual intervention and improv- ing cybersecurity operations. The system incorporates adaptive security mechanisms, a decentralized architecture leveraging federated learning for privacy-preserving collaborative detection, and explainable AI (XAI) for improved interpretability of threat classification. Additionally, adversarial AI defenses are imple- mented to counter sophisticated evasion techniques. Experimental results demonstrate that ATIA significantly improves threat detection accuracy and reduces response time, offering a scalable and proactive approach to modern cybersecurity challenges.

Keywords

Cyber Threat Intelligence, AI, Machine Learning, NLP, SIEM, Adaptive Security, Federated Learning, Explainable AI, Zero Trust, Adversarial AI.